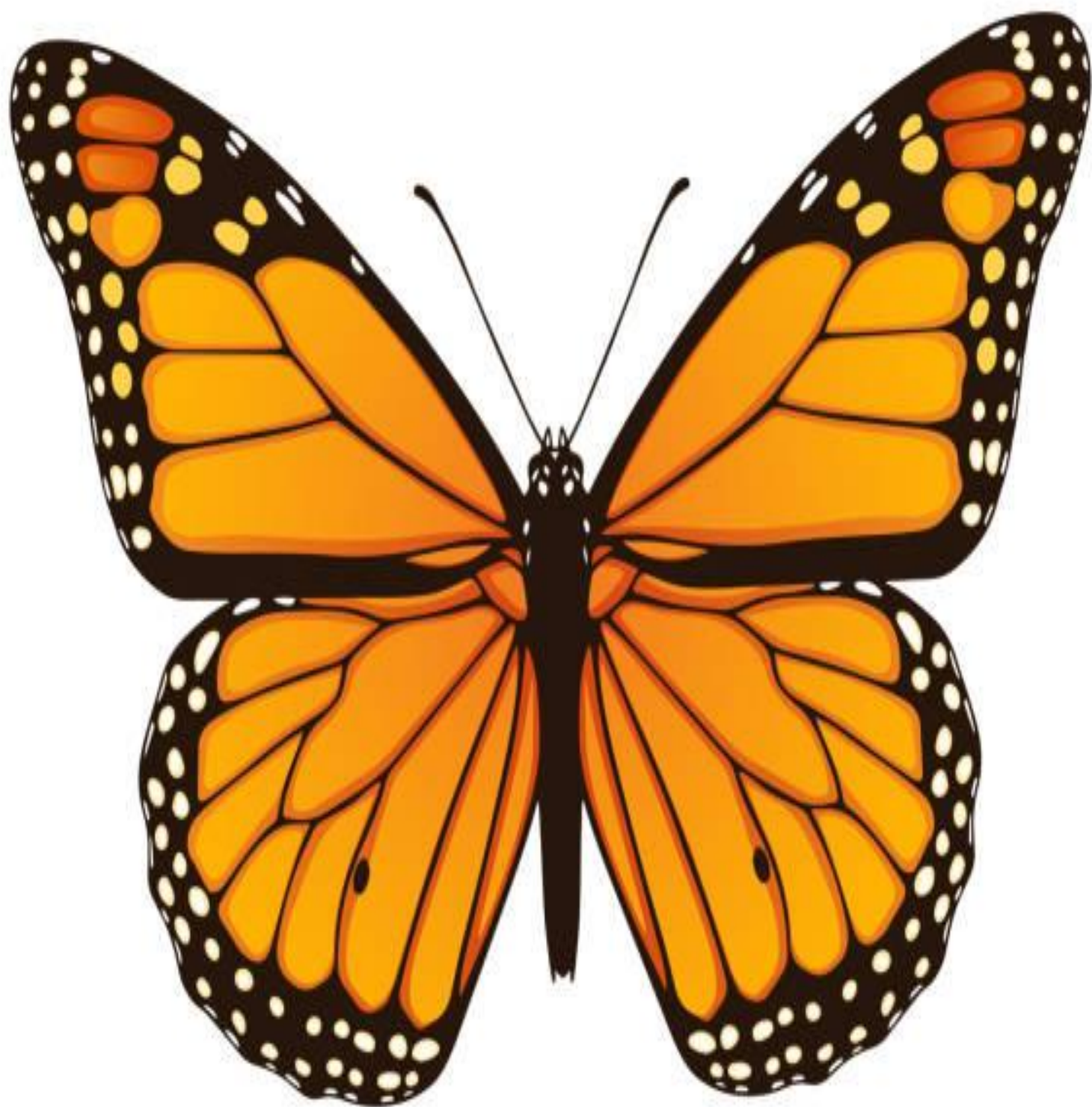




Groups, Rings and Fields

In progress...

Mohammed Fulano

B.Sc. in Applied Mathematics

Algeria

2018

mohammedfulano@hotmail.com

These notes turn around the principal algebraic structures and some of their applications in some subjects like mathematics and physics. They are important structures with a lot of applications, of which we will see some. Psychologically students find them difficult to digest because they are usually introduced without motivation.

The word “*algebra*” comes from Arabic word الجبر .It was used by mathematician Muhammed¹ Al-Khawarizmi(781 – 847) in his book entitled² :

الكتاب المختصر في حساب الجبر والمقابلة

The book was on :

- solving algebraic equations: $ax + b$ and $ax^2 + bx + c = 0$.
Where a, b and c are positive integers.
- the evaluation of some areas and volumes.
- the solution of inheritance problems.

Literally, the word الجبر means “to splint” , in this context it means “to fill in”, meaning the addition of the same term to the two sides of an equation. The word المقابلة means “to confront”, so it can mean “to oppose with another subtraction”, it is the subtraction of the same term from the two sides of the equation , and both operations aim at solving the equation. which means the with two equation to find the solution. The book was transmitted to Europe and translated



Book manuscript

by Italian Gerard **Cremona**(1114 – 1187) and الجبر became *algebra*. Afterwards , Italian **Fibonacci**(1114 – 1187) wrote his book on algebra and doing so , he introduced and popularized the words : algebra , algorithm (the Latinized of Al-Khawarizmi) and Arabic numerals.

Classical Algebra has for study the solution of algebraic equations. After quadratic equations, algebraists attacked the equations of degree 3, 4 and 5. After the work of **Galois** (184 – 1832)a new type of investigations took place and a new discipline added to mathematics under the name

¹ Khwarizmi from Khwarizm, nowadays a region shared between Turkmenistan and Uzbekistan.

² In English “ *The Concise Book of Splinting and Confrontation Calculus*”.

Abstract or Modern Algebra. So, Abstract Algebra is the theory of operations on abstract objects also called mathematical beings. Mathematicians try to go from concrete examples to the general theory.

These following three chapters are extracted from my draft *Number theory, Ideas and Concepts*(2018), I think that no serious prerequisites are needed to read, understand the text and solve the exercises. If there are any mistakes there are still mine, no one is perfect.

Groups

Sets :.....	1
Definition of a group :.....	1
Generators of group :.....	1
Product of groups:.....	1
Free groups :.....	1
Torsion groups :.....	1
Cyclic groups:.....	1
Subgroups :.....	1
Group Representation :.....	1
Lie Groups :.....	1
Galois theory :.....	1
Groups and symmetry :.....	1

Rings

Ring definition :.....	1
Integral domains:.....	1
Matrices :.....	1
Ideals :.....	37
Polynomials :.....	1
Modules :.....	1

Fields

Definition of a Field:.....	1
Finite fields :.....	1
Vector Spaces :.....	1

Linear maps :.....	1
Linear equations revisited:.....	51
Algebras :.....	51

Groups

The theory of groups is very important in mathematics to the extent that French scientist Henri Poincaré (1854 – 1912) said once: “*Mathematics are a matter of groups*”. The concept of group is already present in the work of German Carl Gauss (1777 – 1855) at the beginning of the XIX century. Today this concept is present everywhere, even in physic as well as psychology. So algebra before modern revolution was the science of equation solutions. So to break the psychological barrier, it is perhaps comforting to say that these structures are not invention but discoveries.

○ Sets:

A group is a set. A set E is a collection of objects defined by a certain rule. If E is finite, the number of its elements is noted $\# E$. A function(or a map) is a relation between two sets:

$$\begin{aligned} f : E &\longrightarrow F \\ x &\longmapsto f(x) \end{aligned}$$

A map $f : E \longrightarrow F$ is injective (one to one) if $f(x_1) = f(x_2) \implies x_1 = x_2$. If $E \subset F$, the map is a canonical³ injection and is noted $E \hookrightarrow F$. f is surjective (onto) if $\forall y \in F \exists x \in E : f(x) = y$. If f is both injective and surjective, we call it bijective (one to one and onto), so there is a bijection between the sets E and F and if the sets are finite we have: $\# E = \# F$. If f is bijective then there is an inverse f^{-1} such that $f \circ f^{-1} = id_E$ and $f^{-1} \circ f = id_F$.

○ Definition of a Group:

³ Canonical in many in mathematics means natural, so

A group is a set G with a law of composition $*$ (or binary operation) between its elements that verifies certain rules called axioms⁴.

Definition:

- $-\forall g_1, g_2 \in G : g_1 * g_2 \in G.$
- $-\forall g_1, g_2, g_3 \in G : g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3.$
- $-\exists e \in G, \forall g \in G : g * e = e * g = g.$
- $-\forall g \in G, \exists g^{-1} : g * g^{-1} = g^{-1} * g = e.$

The first axiom means that $*$ is internal or G is closed for $*$. There are interesting composition laws that are not internal like the scalar product. The scalar product of two vectors $a \circ b$ is a scalar (a number). We know that $a \circ b = \sum a_i b_i$ and $|a \circ b| = |a| \cdot |b| \cdot |\cos(\alpha)|$. Whereas the vector product is internal : $a \times b$ is a vector. We have : $|a \times b| = |a| \cdot |b| \cdot \sin(\alpha)$. The cross product $v_1 \times v_2$ is neither commutative nor associative.

We call $g_1 * g_2$ a word. We observe that any $g_1 * g_2 * \dots * g_n$ (or more precisely $g_1^{a_1} * g_2^{a_2} * \dots * g_n^{a_n}$) where $a_1, \dots, a_n$ are integers, is a word in G . So $g^{-1} * g^{-1} * \dots * g^{-1} = g^{-n}$ is a word too.

A group is also noted $(G, *)$ or (G, e) . In what follows we write $g_1 g_2$ in place $g_1 * g_2$ for simplicity. To eliminate the psychological barrier to the reader, we say that the concept of "group" is not an "invention" but a "discovery". The first group saw light under the hands **Gauss**. Later the concept was used independently by French Evariste **Galois** (1811 – 1832) in his work on the roots of algebraic equations. For a lot of time, mathematicians were busy to solve polynomial equations⁵ of the form

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$$

by radicals, which means the solution in term of the coefficient $a_0, \dots, a_n$. they succeeded for $n = 1, 2, 3$ and 4. **Girard** (1 – 1) that every equation of degree n should have exactly n solution a , whose proof waited for **Gauss**

Gauss Theorem

Every algebraic equation of degree n has n roots in $\mathbb{C}$.

⁴ As usual as in mathematics theories, the axioms should be independent (non redundant) and do not lead to a contradiction.

⁵ called also algebraic equation, a solution of an algebraic equation is an algebraic number. The set of algebraic numbers is noted $\mathbb{A}$ which we will see later.

The case $n = 5$

$$a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$$

known as the quantic has proven to be difficult. After the work of **Lagrange**(1736 – 1813) on his roots permutations and resolvent, Italian mathematician Paolo **Ruffini**(1765 – 1822) and Norwegian mathematician Niels **Abel**(1802 – 1829) in 1824 could prove the impossibility of the quantic by radicals, and **Galois** could find the conditions that an algebraic equation has a solution : He discovered three conditions on the set of permutations of roots:

- There is an identity permutation.
- If a and b are permutations then ab is also a permutation.
- Every permutation a has an inverse a^{-1} .

The idea for the proof is to associate to every equation $P_n(x) = 0$ a group and the result:

Theorem

An algebraic equation $P_n(x) = 0$ is solvable in radicals if its group is solvable.

The work of **Galois** and his new ideas would be discovered later by French Camille **Jordan**(1738 – 1922) who discussed the work in his book *Treatise of Substitutions and Algebraic Equations*(1870). Before that, we know that **Gauss** had already considered such group structure in his celebrated book in number theory. **Gauss** showed that the cyclotomic equation $x^n - 1 = 0$ can be solved by radicals. it is called cyclotomic because its solutions which are of the form $a + ib$ divides the circle in n equal parts.

Remarks:

- It was English Arthur **Cayley**(1821 – 1895) who gave the first definition of an abstract group in 1854, then came German Walter von **Dyck**(1856 – 1934) also in his paper(1882).
- The word group was coined by French mathematician Augustin **Cauchy**(1789 – 1859) in 1815. The concept of group as a tool in mathematics become also an independent theory in modern algebra with its autonomous subjects of study like the classification problem of finite groups.
- If the number of elements of G is finite, we say that G is of finite order and we note this number by $\# G$, the notations $|G|$, $Card(G)$ are used too. If not it is a group of infinite order.

— If $g_1 g_2 = g_2 g_1$ for all $g_1, g_2 \in G$, we say that the group G is commutative or Abelian⁶. Almost all groups we treat here are commutative. Even if G is non abelian we have always for every element $g \in G : g g^{-1} = g^{-1} g = e$. The neuter e is unique. Abelian groups are more interesting and easier to work with. Note that associativity is weaker than commutativity.



Abel

— If G is finite, we can present it with a table called the Cayley table⁷, as Pythagoras table of multiplication. If G is abelien, the Cayley table is symmetric along the principal diagonal.

We take the following example: in number theory we have $a \equiv b [n]$ if $a = nk + b$ and we note the set of the residue numbers b by the symbol $\mathbb{Z}/n\mathbb{Z}$. The group $(\mathbb{Z}/n\mathbb{Z}, +)$ is an additive abelian group of finite order, and $\#(\mathbb{Z}/n\mathbb{Z}, +) = n$.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Fig. Cayley table for a finite group $(\frac{\mathbb{Z}}{4\mathbb{Z}}, +)$.

The set $(\mathbb{Z}/n\mathbb{Z}, \bullet)$ is not a group, it is a group when n is prime▲

Examples

— The first group ever studied is the finite set of substitutions (special case of transformations) studied by Lagrange and Cauchy. A permutation is a bijection from E to E . Take a set E of n elements and perform a product noted $*$ (a composition) of possible. Let take the example $n = 2$.

$$\begin{aligned}(a, b) * (b, a) &= (b, a) . \\ (b, a) * (a, b) &= (b, a) . \\ (a, b) * (a, b) &= (a, b) . \\ (b, a) * (b, a) &= (a, b) .\end{aligned}$$

The product here mean rearrangement of the elements a and b . so

⁶ The expression is by French Camille Jordan in honor of Norwegian mathematician Niels Abel and his work in the domain of algebraic equations. Abel wrote the expression $f(g(x)) = g(f(x))$.

⁷ Due to English Arthur Cayley in 1854.

- the composition of two substitutions is a substitutions.
- the composition is associative, for example $((a, b) * (b, a)) * (b, a) = (a, b) * ((b, a) * (b, a)) = (a, b)$.
- (a, b) is the neuter substitution.
- Every substitution has an inverse.

In fact, Lagrange work was based on the permutations of the roots of an algebraic equation. We see that the group S_2 has two elements, e is (a, b) and the group is abelian. S_2 is a group called permutations group. Let take the example $n = 3$. We have 6 (3!) permutations

$$(a, b, c), (a, c, b), (b, a, c), (b, c, a), (c, a, b), (c, b, a) .$$

(a, b, c) Is the neuter element e . We can consider 6 examples :

$$\begin{aligned}(a, b, c) * (c, b, a) &= (c, b, a) . \\(c, b, a) * (a, b, c) &= (c, b, a) . \\(c, b, a) * (c, a, b) &= (b, a, c) . \\(c, a, b) * (c, b, a) &= (b, a, c) . \\(a, c, b) * (c, b, a) &= (b, c, a) . \\(c, b, a) * (a, c, b) &= (c, a, b) .\end{aligned}$$

The general case of this group is called the symmetric group S_n . Its order is $n!$. For example in the case of 3 elements a, b and c , the symmetric group S_3 composed of bijections its order is $3! = 6$.

$$S_3 = \{(a, b, c)(a, c, b)(b, a, c)(b, c, a), (c, b, a), (c, a, b)\}$$

We define the product de two substitutions $(c, b, a)(a, c, b) = (c, a, b)$. Only S_1 and S_2 are abelian. The alternating group A_n are abelian for $n \leq 3$.

–A lot of important sets in mathematics are groups for a certain operation, the reader can verify that the followings sets are infinite order groups⁸ (groups of infinite order) : $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}, +)$, $(\mathbb{C}^*, \cdot)$.

– The group $V_4 = \{e, a, b, c\}$ is an abelian group. It's called the Klein group⁹, its law is defined as follows : $a * b = c$, $a * c = b$, $b * c = a$, and $a * a = b * b = c * c = e$.

⁸ And also $(\mathbb{Z}^n, +)$, $(\mathbb{Q}^n, +)$, $(\mathbb{R}^n, +)$, $(\mathbb{C}^n, +)$.

⁹ The letter V is for German "Vier" which means "four", it has 4 elements.

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Fig. Klein group is abelian.

– $E = (\{1, -1\}, \bullet)$ is a group.

– In algebraic topology, mathematicians work with what is known as homotopy groups like the Poincaré group named also fundamental group. It is a group of classes of equivalences. Another important groups are homology groups.

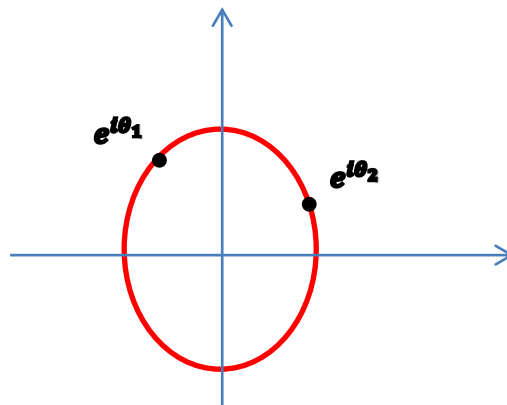
– The set of square matrices A , is an abelian group with as a law of composition $+$.

– The dihedral group :

– the group $\{-1, 1\}$

×	-1	1
-1	1	-1
1	-1	1

– It is to say that the circle is a group! Let's see. The circle for the elements are complex numbers $z = e^{i\theta}$ is indeed a group and the multiplication law $\bullet$ called the circle group noted $C^\times$



$$\begin{aligned}
e^{i\theta_1} \bullet (e^{i\theta_2} \bullet e^{i\theta_3}) &= (e^{i\theta_1} \bullet e^{i\theta_2}) \bullet e^{i\theta_3} \\
e^{i0} \bullet e^{i\theta} &= e^{i\theta} \\
e^{i\theta} \bullet e^{-i\theta} &= e^{i0} = 1
\end{aligned}$$

It is also abelian as $z_1 \bullet z_2 = e^{i\theta_1} \bullet e^{i\theta_2} = e^{i(\theta_1+\theta_2)} = e^{i(\theta_2+\theta_1)} = z_2 \bullet z_1$. This group is topological because $\bullet$ is continuous

—An elliptic curve is a plane curve of the equation $y^2 = x^3 + ax + b$, we can form a group where e is the point at infinity. It is a fruitful group $\blacktriangle$

Subgroup:

Let G be a group. A set $H \subset G$ is a subgroup if

Definition:

- $\forall h_1, h_2 \in H$ we have $h_1 h_2 \in H$.
- $\forall h \in H$ we have $h^{-1} \in H$.

A subgroup H is a group inside another group G . If H is a subgroup in G we note

$$H \leqslant G$$

Remark

- We can simply recapitulate the two conditions by : $\forall h_1, h_2 \in H$ we have $h_1 h_2^{-1} \in H$.
- The subgroups $(\{e\}, *)$ and $(G, *)$ are trivial subgroups of every group G $\blacktriangle$

Examples:

- We have typical examples of subgroups $(\mathbb{Z}, +) \leqslant (\mathbb{Q}, +) \leqslant (\mathbb{R}, +) \leqslant (\mathbb{C}, +)$, $(\mathbb{Q}^*, \bullet) \leqslant (\mathbb{R}^*, \bullet) \leqslant (\mathbb{C}^*, \bullet)$.
- All the subgroups of $(\mathbb{Z}, +)$ are of the form $n\mathbb{Z}$ where $n \geqslant 0$.
- We have also

$$SO(n) \leqslant O(n) \leqslant GL(n)$$

and

$$SU(n) \leqslant U(n) \leqslant GL(n)$$

- Let E be a set and , the set of homeomorphism is included in the set bijections between E and F : $\text{Homeo}(E) \leq \text{Bij}(E)$.
- we have seen the symmetric group . it has in the theory of equation that makes a symmetric group has subgroups so we have

$$G_2 \subset V_4 \subset A_4 \subset S_4$$

and

$$A_n \leq S_n$$

- $\{-1, 1\}$ is a subgroup of $\{-1, 1, i, -i\}$ according the following table:

×	-1	1	i	-i
-1	1	-1	-i	i
1	-1	1	i	-i
i	-i	1	-1	1
-i	i	-1	1	-1

- $\mathbb{C}^\times$ is a subgroup of $\mathbb{C}$.
- we have seen the symmetric group . it has subgroups of order $n!$
- in the symmetric group S_3 above. We define the product de two substitutions $(c, b, a)(b, c, a) = (a, c, b)$. Only two elements are changed it is transposition this set of transpositions is the alternating subgroup noted A_3 it is a subgroup of S_3 ▲

Some important applications

Lagrange¹⁰ theorem:

Let G finite group and H a sub-group of G , then the order of H divides the order of G :

$$\frac{\#G}{\#H} \in \mathbb{N}.$$

¹⁰ **Lagrange** did not the creation of group theory but substitution groups of algebraic equations that Galois has developed afterwards.

The number $\frac{\#G}{\#H}$ is called the index of H in G and noted $[G \div H]$. The coming developments in algebraic structures show that there is a relation between algebraic structures and prime numbers. Let's introduce, the concept of p -group :

Definition:

A finite group G is a p -group iff $\# G = p^n$.

Examples:

—as example $\mathbb{Z}_{p^2}$ is the finite groups : $\mathbb{Z}_4, \mathbb{Z}_9$

Lagrange theorem has a converse : the tow **Cauchy** and **Sylow** theorems.

Cauchy theorem:

Let G finite group and a prime p such that p divides $\# G$, then there exists a subgroup H such that $\# H = p$.

It means also that if p divides $\# G$, then there exist such that $g^p = e$. **Cauchy** proved the theorem for the group of substitutions in 1845. Another related theorem important is the **Sylow** theorem due to Norwegian mathematician Peter **Sylow**(1832 – 1918) in

Sylow theorem:

Let G be a finite group and a prime p such that p^k divides $\# G$, then there exists a subgroup H such that $\# H = p^k$.

So for every prime factor p of the number $\# G$, there exists a subgroup of order p^k . It is the partial converse of **Lagrange** theorem.

The theorem helps in classifying finite groups. English William **Burnside** (1852 – 1927) was a pioneer in finite group theory, he emitted in 1902 conjectures on finite groups, one of them was disproved by Russian mathematician Igor **Shafarevich**(1923 – 2017) in 1964. The Restricted Burnside Problem was proved by Russian **Zelmanov** (1955–)in 1990. The task of classification of finite simple groups was finished only in 2004 after efforts of many mathematicians like English John **Conway**(1937 – 2020).

Another type of structures is the semi-group. If $*$ is closed and associative only, then $(G, *)$ is a semi-group. Semi-groups have application in like differential equations. There is also the problem of classifying semi-groups.

Another concept : We say that an element $g \in G$ is of order k if there exists a least naturel integer

k such that $g^k = e$. If k does not exist, we say that g has an infinite order. If $g^n = e$ then k divides n . If G is finite then k divides $\# G$.

○ Generators of Groups:

We with an operation $*$ and we say : let $(G, *)$ be a group. In some groups, there are relations between elements called the generators of the group. So there are element $S = (g_1, \dots, g_n)$ of G can suffices by the operation $*$ to give(to generate) all the other elements of G , we this by saying that set the generators of the group G and we not that by

$$\langle S \rangle = G$$

Every group has a generating subset. German Walter von **Dyck**(1856 – 1934) was the first to define groups in terms of generators.

Definition:

If there exist $a \in G$ such that $\forall g \in G, \exists k : a^k = g$ and a is the generator. we write

$$\langle a \rangle = G$$

We say that G is monogenic. Bu it is misleading appellation, as a group can have more one than generator.

Let G be a group and $S \subset G$, the subgroup generated by S is defined as $\bigcap_{i=1} H_i$ such that $S \subset H_i$ we note this by

$$\langle S \rangle = \bigcap_{i=1} H_i$$

Examples

— $\mathbb{Z}$ is a group with generator 1. It is monogenic. $a^k = g$ here means $1 + 1 + \dots + 1 = g$. We write $\langle 1 \rangle = \mathbb{Z}$ or $\langle -1 \rangle = \mathbb{Z}$.

— Let the group $\mathbb{Z}$ and $S = \{a_1, \dots, a_n\}$. The subgroup generated by S is $\langle S \rangle = \text{pgdc}\{a_1, \dots, a_n\}\mathbb{Z}$

— $\mathbb{Z}_n$ is a monogenic group. $\mathbb{Z}_n = \langle n \rangle$ ▲

○ Product of Groups:

There are many product concepts in mathematics that are related to our subject:

-The Cartesian¹¹ product of two sets E and F called also direct product of two sets E and F

$$E \times F = \{(x, y) : x \in E, y \in F\}$$

sets. Note that $E \times F \neq F \times E$.

let $G_1, \dots, G_n$ n groups and we want to construct a group G such that all groups $G_1, \dots, G_n$ are subgroups of G . we have two possibilities :

-product of groups:

-Direct product

-Direct sum : $v_1(a, b) \oplus v_2(c, d) = v_3(a, b, c, d)$

-Free product

we here the direct noted $G_1 \times G_2$

Definition

Let two groups : $(G, *)$ and $(H, \blacksquare)$ is $G \times H$ is the set of couples $(g_1 * g_2, h_1 \blacksquare h_2)$.

Remark

—The product of two groups G_1 and G_2 is it is sometimes by direct sum.

—The product of two groups G_1 and G_2 is itself a group. The is associative, there is a neuter elemnt and inverse.

—For finite groups, we have : $\# (G_1 \times G_2) = \# (G_1) \bullet \# (G_2) \blacktriangle$

Examples:

— $\mathbb{Z} \times \mathbb{Z}$ is the Cartesian product , it is the (n_1, n_2) .

— $\mathbb{R} \times \mathbb{R}$ is the product of two groups $(\mathbb{R}, +)$. The elements of the product of the form $(g_1 + g_2, h_1 + h_2) \blacktriangle$

○ Cyclic Group:

^[11] Form the Latinized name of René Descartes(1 – 16).

A finite monogenic group is cyclic. $\frac{\mathbb{Z}}{n\mathbb{Z}}$ is the quotient group of $\mathbb{Z}_n$. Is

Definition:

let $\forall$ a group. The group is cyclic if $\exists g_0 \in G \forall g \in G$ we have $g = g_0^n$ for some integer. We write

$$G = \langle g_0 \rangle$$

Remark

- g_0 is called the generator. It may be not unique.
- if g_0 is a generator of G then g_0^{-1} is also a generator.
- A cyclic group can either finite or infinite.
- Every subgroup of a cyclic group is cyclic.
- A cyclic group is always abelian $\blacktriangle$

Examples:

- $\mathbb{Z}$ is an infinite cyclic group with two generators : $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.
- $\mathbb{Z}_6$ is a finite cyclic group with generators : $\mathbb{Z}_6 = \langle 1 \rangle = \langle -1 \rangle$ $\blacktriangle$

We have the following theorem:

Theorem:

Every finite abelian group is a direct product of cyclic groups.

A result about classification of cyclic groups:

Theorem:

- if G is a group of finite of order n , then it is isomorphic to $\mathbb{Z}_n$.
- if G is a group of infinite then it is isomorphic to $\mathbb{Z}$.

$\bigcirc$ Torsion Groups:

French Henri **Poincaré** (1837 – 1912) introduced the idea of torsion in topology, it is that the Mobius band is a manifold with torsion and the with torsion coefficients hence the torsion group.

Definition:

A torsion subgroup T is a subgroup of G where every element has a finite order : $g^n = e$.

Otherwise for every $g \in G$ there is $n \in \mathbb{N}$ such that $g^n = e$. The torsion of group are all elements such that if only $e^k = e$ we say that G is without torsion. the word torsion comes from **Poincaré** when he considered the torsion coefficients of a manifold.

Remark

— If only e then G is torsion-free group. ▲

Examples:

— $\mathbb{Z}_n$ is a torsion group. ▲

○ Normal subgroups

Let G be a group, and let's define conjugation. We say that a and $b \in G$ are conjugate if there exist $g \in G$ such that $gag^{-1} = b$.

Definition:

Let G be a group and H a sub-group of G . The subgroup H is a normal sub-group iff for every $h \in H$ and $g \in G$ we have

$$ghg^{-1} \in H.$$

mean stht H is closed with respect to the conjugation operation. Now let H be a subgroup of G . H is normal sub-group if

- $HG = GH$.

- $g^{-1}Hg = H$.

- for every $g \in G$: $gH = Hg$.

If H is a normal subgroup of G , we note this by writing: $G \supseteq H$ or $H \trianglelefteq G$. If then we can study H in place of G .

Remark

— A group G is simple if the only normal groups are $\{e\}$ and G . Simple groups are like atoms for groups ▲

Examples:

- Let G be a group, then G and $\{e\}$ are two normal subgroup of G .
- The alternating group A_n is a normal subgroup of symmetric group $S_n : A_n \trianglelefteq S_n$, so the symmetry group S_n is not simple.
- Finite simple groups are now completely classified. There is a monster group the biggest sporadic simple group.
- The alternating group A_n are all simple for $n = 3$ and $n \geq 5$, we have $\# A_5 = 60$.
- The translations subgroup of all isometries of the plane is normal▲

Theorem:

Let G be an abelian group. Every subgroup H of G is a normal.

Proof :



A group in which every subgroup H is normal is called a Dedekind group. A Hamilton group is non abelian Dedekind group. All abelian groups are Dedekind groups.

○ Quotient group:

we first introduce equivalence relation

Definition:

Let E be a set R a relation on E . The relation is an equivalence relation if:

- R is reflexive.
- R is symmetric.
- R is transitive.

An equivalence relation on E creates a partition of E in equivalence classes, meaning that they are disjoint subsets. So the quotient of E with respect to $\sim$ the $E/\sim$ is a quotient. Is G/f .

Examples:

- The operation $=$ is an equivalence relation on $\mathbb{C}$.
 - The parallel operation $//$ is an equivalence relation in the plan $\mathbb{R}^2$.
 - Let $E = \mathbb{Z}$ the operation $\sim$ defined as $n_2 - n_1$ is even is an equivalence relation $E/\sim = \{0,1\}$.
- ▲

With a subgroup H of a group G we can construct a new structure. Normal subgroups we can construct a new structure which is quotient group.

Definition:

Let G be a set N a relation on E . quotient group and noted G/H the quotient group is the set of all cosets.

Remark

- The concept and term “quotient group” was introduced by French Camille **Jordan** (1838 – 1922) in 1873.
- a quotient group is the set of coset Hx ▲

Examples:

- Let $G = \mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ noted also $\frac{\mathbb{Z}}{n\mathbb{Z}}$ is the quotient group of $\mathbb{Z}_n$. The coset are
- the projective group is the quotient group of the linear group $GL()$ ▲

○ Free Groups:

A free group is group without relations.

Definition:

Let G be a group. a free group G .

Remark

- The name free was coined by Danish Jacob **Nielsen** (1890 – 1959) in 1924
- a free group cannot be finite except the trivial free group ▲

Examples:

- $\mathbb{Z}$ is a free group with generator 1.
- the Klein group is not free.
- is a free group with generator 1 $\blacktriangle$

Dedekind proved that every subgroup of an abelian free group is free then another result

Nielsen-Schreier Theorem:

Any subgroup H of a free group G is free.

Proved by Danish Jacob **Nielsen** (1890 – 1959) and German Otto **Schreier** (1901 – 1929) in the years 1921 – 1926.

Theorem:

Any group G is a quotient of a free group.

the Free product $*$ we have for example $\mathbb{Z} * \{e\} = \mathbb{Z}$

○ Homomorphism of Groups:

As we can have maps (a map is a relation between two sets) f from a set E to another set F . Mathematicians have discovered that a lot of maps between structure are morphisms. Some morphisms is called morphism. A morphism (a general term) is from Greek $\mu\omicron\rho\phi\eta$ meaning “form” and so a morphism is the state of having a form. A morphism is a map that preserves the structure. We can have morphisms between sets. The morphism between two groups is usually called homomorphism. Many in of mathematics like algebraic topology, are homomorphism due to the importance of the concept.

We can consider the composition law of a group as a map

$$\begin{aligned} *: (G, *) &\times (G, *) \rightarrow (G, *) \\ g_1 * g_2 &\rightarrow g_3 \end{aligned}$$

So a homomorphism is

$$\phi: (G_1, *) \rightarrow (G_2, \blacklozenge)$$

$$\phi(g_1 * g_2) = \phi(g_1) \diamond \phi(g_2)$$

— Isomorphism : ϕ is a homomorphism and it is bijective and the ϕ^{-1} exists.

$$\begin{aligned}\phi^{-1} : (G_2, \diamond) &\rightarrow (G_1, *) \\ \phi^{-1}(g_1 \diamond g_2) &= \phi(g_1) * \phi(g_2)\end{aligned}$$

An interesting is that two groups can isomorphic. It is the isomorphism problem which is a central problem in group theory.

— automorphism : it is an isomorphism the bijection from E in itself from E into E .

A morphism group is $\phi: (G, e_1) \rightarrow (G, e_2)$. Such that $\phi(g_1 g_2) = \phi(g_1) \phi(g_2)$. For every homomorphism ϕ of groups, we can define two sets :

— the kernel : noted $\ker$ and defined as

$$\text{Ker}(\phi) = \{g \in G_1 : \phi(g) = e_2\}$$

It measures the injectivity of ϕ . We can prove that is a subgroup of E .

— the image : of ϕ is defined as

$$\text{Im}(\phi) = \{g \in G_2 : \phi(g) = g\}$$

If two finite groups G_1 and G_2 are isomorphic then $\# G_1 = \# G_2$. We have an important result

Theorem:

Let G be a group and ϕ a homomorphism

$$\text{Im}(\phi)G \leqslant G \quad , \quad \text{Ker}(\phi) \triangleleft G$$

American Garrett **Birkhoff** (1911 – 1996) said : “...One may even describe abstract algebra as the study of those proprieties of algebraic systems which are preserved under isomorphism”.

Remark

— If two groups G_1 and G_2 are isomorphism they have the same proprieties : if G_1 is commutative then G_2 is commutative too,...

— in the *theory of category*¹² if $f = \text{Ker } \phi$ is a monomorphism and in category theory functors and categories. If $F = \text{Im } f$ we say that f is an epimorphism.

Category theory is a general view to abstract algebraic structure and their machinery, for example there are similarities in set theory, topology, algebra,... it is not so necessary to understand those branches of mathematics but its primary goal is to organize and unify the language. A category is a of objects between which we define morphism called arrows. A collection of sets, groups, topological spaces,...and are homomorphism, maps continuous maps,... respectively



so

Category	Functor
set	map
Vector space	Linear map
Topological space	Continuous map
group	homomorphism
...	...

If ϕ is mono and epimorphism we say that is an isomorphism. An isomorphism is a bijective homomorphism ▲

Examples:

— Linearity is a morphism between two vector spaces which are groups $(V, +)$

$$f : (\mathbb{R}, +) \rightarrow (\mathbb{R}, +)$$

$$f(x + y) \rightarrow f(x) + f(y)$$

V here is $\mathbb{R}$. $\ln(x)$ is a homomorphism of groups $(\mathbb{R}, +)$, e^x homomorphism of, the determinant $\det(A)$ is homomorphism of groups $GL()$.

— $f(x) = x^2$ is a morphism between two groups $(\mathbb{R}, \bullet)$

$$f : (\mathbb{R}, \bullet) \rightarrow (\mathbb{R}, \bullet)$$

$$f(x \bullet y) \rightarrow f(x) \bullet f(y)$$

¹² Category theory was created principally by Samuel Eilenberg(1913 – 1998) and Saunders MacLane(1909 – 2005) around 1950 to the abstract homology algebra.

— both $(\mathbb{R}^{*+}, \cdot)$ and $(\mathbb{R}, +)$ are isomorphic groups, the homomorphisms are $\log(x)$ and e^x .

— the morphism between

$$\begin{aligned} f: \mathbb{Z} &\rightarrow n\mathbb{Z} \\ f(n) &\rightarrow nk \end{aligned}$$

Is an isomorphism.

— with mod n we define the homomorphism

$$\begin{aligned} f: \mathbb{Z} &\rightarrow \mathbb{Z}_n \\ f(n) &\rightarrow \text{mod } n \end{aligned}$$

It is not an isomorphism.

— isometrie (that preserve measurements) homomorphism $\blacktriangle$

There is an important result about isomorphism due to English algebraist Arthur Cayley (1821 – 1895).

Theorem:

Let G be a group. Every group is isomorphic to a subgroup of the symmetric group S_n .

F

○ Action Groups:

We introduce here the concept of group action on a set X which can be a topological space (manifolds...) or can be a group itself. This is used for example in algebraic topology to define quotient space. So when transformation a groups acts on the point of a manifold and the can be different.

Definition:

Let G be a group and X a set. We define a map

$$\begin{aligned} &: G \times X \rightarrow X \\ (g, x) &\rightarrow x \blacklozenge g = y \end{aligned}$$

With the proprieties:

$$\begin{aligned} -g_1 \blacklozenge (g_2 \blacklozenge x) &= (g_1 g_2) \blacklozenge x \\ -\forall x \in X: e \blacklozenge x &= x \end{aligned}$$

The space X is called a left G-coset (g in $\blacklozenge g$, is at the left side) and by the same manner we define the right G-coset.

Remark

- Every group acts on itself. It is a *translation* action.
- If X is a right G -coset it does not mean necessarily that it is a left G -coset. If G is abelian we have : $GX = XG$.
- The action of G on X form a partition of X and thus an equivalence relation : $x \sim y$.

Examples:

- Let $G = \mathbb{Z}$ and $X = \mathbb{R}$, we define an action of $\mathbb{Z}$ on $\mathbb{R}$ such that $n \blacklozenge x = n + x$.
- Let $X = V$ a vector space the scalars of the field acts on the vectors of the vector space by scalar multiplication.

Orbit

When G acts on a space X , the set of all y resulting from the operation on an element $x \in X$. it is the orbit of x by the elements of G

$$Orb_x = \{y : g \blacklozenge x = y\}$$

The cardinal of the orbit Orb_x is the cardinal of G .

Theorem

The set $\bigcap_1^n St_x$ forms a normal subgroup of G .

Action of a Subgroup on a Group:

We an action in place of G one of its subgroups and when X is G itself .

Definition:

Let G be a group and H a subgroup of G . We define a map

$$\begin{aligned} * : H \times G &\rightarrow G \\ (h, g) &\rightarrow h * g = hg \end{aligned}$$

Remark

- Every subgroup H acts on G . In this case $\blacklozenge$ is simply $*$.
- if a subgroup H acts on G then the cardinal of the orbit is the order of H $\blacktriangle$

Examples:

— Let $G = \mathbb{Z}$ $\blacktriangle$

Conjugated action

Let G and H a subgroup.

Definition:

Let G be a group and H a subgroup of G . We define an action of H on G as follows

$$= \{y : g * h * g^{-1}\}.$$

The action is noted gHg^{-1}

Stabilizer

Let G acting on X . the stabilizer of G is such that $St_x = \{g : gx = x\}$.

Remark

— If $St_x = \{e\}$ then the action is free or G acts freely on X .

— if $\bigcap St_x = \{e\}$ then the action is effective $\blacktriangle$

Examples:

— An example of a free action is of a group G acting on itself $ge = g$ $\blacktriangle$

We have

We say is a if

$$\# G = \# (Orb) \cdot \# (St_x)$$

h

Theorem

The action is free $\Rightarrow$ the action is effective

The action is effective $\nRightarrow$ the action is free

Center

Let G acting on a space X . The center of G is such that $Z(G) = \{g : gx = x\}$. We

$$|\# G| =$$

s

when X is a G –set there is projection called canonical projection

$$\pi : X \rightarrow X/G$$

○ Topological Groups:

We have seen groups like the with is that the composition is continuous and other discontinuous.

Definition:

Let $(G, *)$ be a group. If the law $*$ is continuous, the group is called topological.

Examples:

–the

– $(\mathbb{Z}_2, +)$ ▲

Other group called classical by German Herman **Weyl**(18 – 19) in his book *The Classical Groups, their Invariants and Representations* (1939) and also French Jean **Dieudonné**(19 – 199) in his book *Sur les Groupes Classiques*(1948).

○ Representation of Groups:

Here we will discover a link between groups and linear algebra. To get information on a group G we can use representation. The idea was first by German **Frobenius**(18 – 19) in 1896. he by German Richard **Dedekind**(18 – 191) Can be in finite group, for infinite can be very hard.

Let G be a group and V a vector space. A representation of G on the vector space V consists in a homomorphism:

$$\varphi : G \rightarrow GL(V)$$

where linear map from V to V (at the same time matrices). the homomorphism respects the group structure : $\forall \varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2)$.

The idea is to represent a group G by a matrix. Representation group, is a homomorphism group to $GL(\mathbb{C})$ of matrices, in this acts on $\mathbb{C}$ with matrices.

Examples:

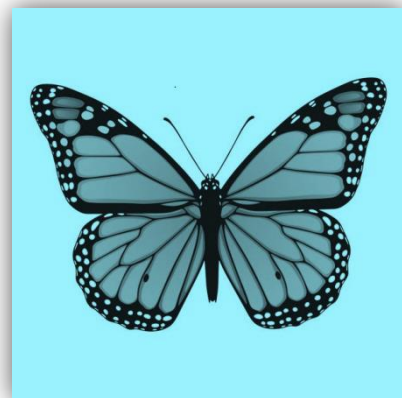
– the trivial representation: let G be any group, this $\forall g \in G$ we have $\varphi(g) = 1$. So $\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) = ee = e$.

– $(\mathbb{Z}_2, +)$ on $\mathbb{C}^{\blacktriangle}$

○ Groups and Symmetry:

Mathematicians have discovered two important concepts in mathematics and physics : those of duality and symmetry. For example, the complex roots of an algebraic equation are symmetric to the real axis.

The one the more associated with the group structure is : symmetry, and we have seen this with geometry. The idea of using group in geometry is very original and was first by German mathematician Felix Klein (1849 – 1925) in 1872.



How many axes of symmetry are there?

In fact the concept of group is intimately linked to symmetry. Klein had to in the university of Erlangen (of Germany) and he proposed a program that to classify geometry by the idea of transformation groups

The geometry is characterized by the group of transformations that preserve elementary properties

This philosophy was following the of geometry in the XIX century and invention of hyperbolic and parabolic, projective,... geometries. Discrete symmetry:

More is to consider a group which has for elements symmetries. An example is the operation of a triangle, a tetrahedron

continuous symmetry: the $SO(n)$ group of continuous so they are topological.

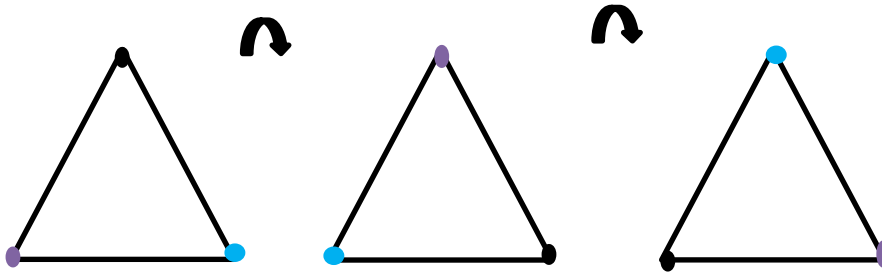


Fig. 3 rotations

The set of isometries that preserve regular n -polygon forms a group: the dihedral group of order $2n$ noted D_n . For $n = 3$ it is triangle we have 3 rotations and 3 reflexions..

We know that the congruence n modulo n correspond to rotations of $\frac{2\pi}{n}$ an isomorphism.

Physics:

The theory of group is very rich in applications. In physics, physicists found a power tool which is group theory. In particle physics, symmetry plays a very important to predict the existence of new particles. The Dirac equation has two solutions : the particle –the antiparticle. When a particle collides with an antiparticle they annihilates each other giving energy(photon) look like $gg^{-1} = e$. Gauge theory was initiated by German scientist Herman¹³ **Weyl**(1885 – 1955). Physicists began to build upon the ideas¹⁴.



Weyl

The intertwining of symmetries of physics is in groups matrices :

$U(1)$: unitary group

$SU(2)$: special unitary of matrices of order 2

$SU(3)$: specila unitary of matrices of order 3

So the standard model of particles to the group is $U(1) \times SU(2) \times SU(3)$.

A by German mathematician Emmy **Noether**(18 – 193) That the laws of nature have underlying symmetries that their conservation.

Noether theorem(1915):

Conservation of the angular momentum from the symmetry(isotropy) of time.

Conservation of the electromagnetic charge from the gauge symmetry.

Conservation of energy from the symmetry(homogeneity) of time.

Conservation of linear momentum from the symmetry(homogeneity) of space.

¹³ His ideas on also his book : *Group Theory and Quantum Mechanics*(1931).

¹⁴ As Steven Weinberg paper(1967) : “A Model of Leptons”.

metri

○ Lie Groups:

One of symmetry are Lie groups. In 18, Norwegian mathematician Sophus Lie (18 – 18) on that in geometry are groups. He used linear algebra. As Galois used solvable groups to solve algebraic equations Lie thought he could use groups to solve differential equations.

A Lie group is both a group and a manifold.

Examples:

—The general linear group $GL(n, \mathbb{R})$ (or $GL(n, \mathbb{C})$) and its two subgroups. The is smooth manifold because the matrix product is smooth.

—The $SU(n)$ is the special group consisting in unitary U such that $\det(U) = 1$.



Exercises

- 1) show that $0, 1, \frac{1}{2}$ and $\sqrt{2}$ are algebraic numbers.
- 1) show that $f(x) = x + 1$ is injective. Is $f(x) = \cos(x)$ injective ?
- 1) let $f(x) = x + 1$ and $g(x) = x + 1$.
—compare between $f \circ g$ and $g \circ f$.
—Let $g(x) = x^2$. Compare between $f \circ (g \circ h)$ and $(f \circ g) \circ h$.
- 1) let $f(x) = x^2 - 1$ and $g(x) = x^2 + 1$. Find $f \circ g$ and $g \circ f$.
- 1) is $\emptyset$ a group?
- 1) show that e is unique .
- 1) Show that S_3 is not abelian.
- 1) let G a group where for every $g \in G : g^2 = e$. Show that G is abelian.
- 1) show that the neuter e is a neuter from right and from left.
- 1) show that a right inverse is also a left inverse.
- 1) show that the inverse g^{-1} is unique.
- 1) show that $|a \times b|^2 = |a|^2 |b|^2 - |a \circ b|^2$.
- 1) show that the product $a \circ b \times c$ does not need parentheses.
- 1) G is a group such that $\forall x \in G : x^2 = e$, show that G is abelian.
- 1) Are $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ groups?
- 1) show that $(\{1, -1, i, -i\}, \cdot)$ is a group. Draw its Cayley table.
- 1) Is the matrices set with matrix multiplication a group?
- 1) Is $(\mathbb{Q}^*, +)$ a group ?
- 1) show that the set $(\frac{\mathbb{Z}}{3\mathbb{Z}}, \cdot)$ is a group, and draw its Cayley table.

- 1) why are $(\mathbb{Z}^{*n}, \bullet), (\mathbb{Q}^{*n}, \bullet), (\mathbb{R}^{*n}, \bullet), (\mathbb{C}^{*n}, \bullet)$ not groups ?
- 1) show that the operation in the circle group $C^\times$ is internal.
- 1) Show that $(\{e\}, *)$ is a group. It is the trivial group.
- 1) Let $H \leq G$. Show that $e \in H$.
- 1) let G a cyclic group, show that G is abelian.
- 1) If g_0 is a generator of G then $-g_0$ is also a generator
- 1) Let H_i subgroups of G . Show that $\cap H_i$ is a subgroup of G .
- 1) Determine all subgroups of group of prime order p .
- 1) Show that $\{e\}$ and G are normal subgroup of G .
- 1) show that every subgroup H of an **abelian** G is normal.
- 1) let $f : G_1 \rightarrow G_2$ be a homomorphism. Show that the kernel of f normal subgroup of G_1 .
- 1) Let H a normal subgroup of G . Show for every $g \in G : gH = Hg$.
- 1) Show that the operation $=$ is an equivalence relation on $\mathbb{C}$.
- 1) Show that the parallel operation $//$ is an equivalence relation in the plan $\mathbb{R}^2$.
- 1) Show that the composition law in $O(n)$ is internal.
- 1) Let ϕ a homomorphism of groups G and G' , show that : $\phi(e_1) = e_2$
- 1) show that : $\phi(g^{-1}) = (\phi(g))^{-1}$.
- 1) Let f linear, show that $f(0) = 0$.
- 1) Show that $\equiv$ in $\mathbb{Z}_n$ is an equivalence relation. There is a canonical projection $\pi : \mathbb{Z}_n \rightarrow \mathbb{Z}_n / \equiv$
- 1) why $f : \mathbb{Z} \rightarrow \mathbb{Z}_n$ is not an isomorphism ?
- 1) Show that the map $\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$ is not an isomorphism.

Rings

The origin of the ring concept is the set of integers $\mathbb{Z}$. The set $\mathbb{Z}$ is a classical central set in number theory with a lot of investigations on integers like : divisors, prime numbers,...so a general ring $(\mathcal{R}, *, \diamond)$ in abstract algebra is a structure like $(\mathbb{Z}, +, \bullet)$ where we look for what is in $\mathbb{Z}$: integers , prime numbers,....

In what follows we study the concept of general ring. So we will see rings not necessarily like $\mathbb{Z}$ but may lack some good properties.

○ Definition of a Ring:

Definition:

$(\mathcal{R}, *, \diamond)$ is a ring if

— $(\mathcal{R}, *)$ is an **abelian** group.

— $\diamond$ is associative : $\forall x_1, x_2, x_3 \in H$ we have $x_1 \diamond (x_2 \diamond x_3) = (x_1 \diamond x_2) \diamond x_3$.

— $\diamond$ is distributive over $*$: $\forall x_1, x_2, x_3 \in H$ we have $x_1 \diamond (x_2 * x_3) = (x_1 \diamond x_2) * (x_1 \diamond x_3)$.

So in a ring $(\mathcal{R}, *, \diamond)$, we have two laws of composition. The first is composed of a group $(\mathcal{R}, *)$ which is **abelian**, and the second $(\mathcal{R}, \diamond)$ which is not necessary a group. We can say that a ring is composed of

— $(\mathcal{R}, *)$ which is an **abelian** group.

— $(\mathcal{R}, \diamond)$ which is a semi-group.

— the operation $\diamond$ is distributive on $*$.

Remark:

- The word “ring” was introduced by German mathematician David Hilbert¹⁵(1862 – 1943) in 1892. German mathematician Richard Dedekind (1831 – 1916) used the word domain.
- the theory of rings were very studied and developed further mainly by Germans Emmy Noether(1882 – 1935) and Emil Artin(1898 – 1962)
- A ring can be finite or infinite.
- If the operation $\diamond$ is commutative, the ring is a commutative (or abelian)ring $\blacktriangle$

Examples:

- A trivial ring is $\mathcal{R} = \{0\}$.
- the set of matrices A with $+$ and $\bullet$ as the two composition laws is a ring. It is not commutative, we will see more information on it.
- both $(\mathbb{Q}, +, \bullet)$ and $(\mathbb{R}, +, \bullet)$ are commutative rings.
- the set $(\mathbb{Z}/n\mathbb{Z}, +, \bullet)$ is a ring, it is commutative, the operation $\equiv$ defines an equivalence relation in the ring $\blacktriangle$

Unitary rings:

The previous definition of a ring is general.

Definition:

if there is a neuter element e for $\diamond$ such that $a \diamond e = e \diamond a = a$, we say that $(\mathcal{R}, *, \diamond)$ is unitary ring.

Examples:

- $(\mathbb{Z}, +, \bullet)$ is a unitary ring .
- the set of matrices $\mathcal{M}$ with operation $+$ and $\bullet$ is a unitary ring.
- the set $(\mathbb{Z}/n\mathbb{Z}, +, \bullet)$ is a unitary ring $\blacktriangle$

Any element of the ring such that $aa = aa = 1$ is called a unit or invertible element. A characteristic of a ring is an integer such that $a^n = 1$. If $n = \infty$ is it is 0. Homomorphism of a ring .

$$\phi : (\mathcal{R}, *) \rightarrow (\mathcal{R}, \diamond)$$

$$\phi(g_1 * g_2) = \phi(g_1) \diamond \phi(g_2)$$

¹⁵ And used it in his book *Algebraic Theory of Number Fields*(1897).

○ Matrices

We see now an important unitary ring : the ring of matrices $\mathcal{M}$ known to undergraduate students. Matrices are used in a lot of mathematical applications. In modern mathematics language, matrices are seen as objects like numbers, functions,... A matrix of order $n \times m$ is a matrix of n rows and m columns. A matrix of $n \times n$ is a matrix of n rows and n columns, it is a squared matrix of order n . Squared matrices are far very important in applications. A matrix can be noted by one of the following symbol

$$\| \quad \|, \quad (\quad), \quad [\quad]$$

they can be of finite order like the 2×2 matrix $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ or of infinite order like

$$\begin{bmatrix} a_{11} & \cdots & \\ \vdots & \ddots & \vdots \\ & \cdots & \end{bmatrix}$$

the latter has an infinite number of rows or columns. We can find in physics a complex matrix

$$\begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix}$$

We can perform between matrices well defined operations as

$$AB, \quad A + B, \quad A - B, \quad \alpha A$$

The operations $A + B$, $A - B$, αA commute, but the product of matrices may be not commutative so in general : $AB \neq BA$. We will see for some matrices we have $AB = 0$ without A or B is zero. An invertible matrix A if there exists a matrix B such that $AB = I$. not all matrices are invertible.

Using the addition between (n, m) matrices we observe the same algebra as in numbers. So the collection of $n \times m$ matrices is an additive group¹⁶.

Groups of matrices:

Talking on a group of matrices, there are other useful groups of matrices:

¹⁶ in fact any set of $n \times m$ matrices is a group for +.

- The collection of $n \times n$ invertible matrices is a group called $GL_n(\mathbb{R})$. It is not **abelian**.
- The **Euclidian** group is the group of translations, reflection and rotations in the **Euclidian** space (like $\mathbb{R}^n$)
- The **Heisenberg** group is the group of 3×3 matrices of the form $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$, the composition law is the usual matrix multiplication.

Remark

- a unit or invertible element in the set of matrices is a matrix that has an inverses. such that $AA^{-1} = A^{-1}A = I$



Linear systems:

A linear system is a collection of linear equations

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\dots\dots\dots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

of m equations with n unknowns. These systems naturally stem from many practical situations. Consider we point in the plan $(x_1, y_1), \dots, (x_n, y_n)$ and a polynomial $P_{n-1}(x)$ that passes on the points (curve fitting) so we get

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\dots\dots\dots \\ a_{11}x_1 + a_{11}x_2 + \cdots + a_{11}x_n &= b_n \end{aligned}$$

matrix is a tool and in place of linear systems. To a linear system of equations, we use a matrix

$$AX = Y$$

where Y is a given vector and X the unknown vector. A matrix is just the coefficients a_{ij} in the

linear system so study the linear system it suffices to study the matrix. A matrix A transforms a vector v_1 to another vector v_2 .

Any linear has infinitely many solutions. If add equation we add constraint to the system and the number of possible solutions diminishes.

The product of matrices can be between two of the different order

$$\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} \begin{bmatrix} g & h \\ i & j \\ k & l \end{bmatrix}$$

There is a special matrix that plays the role of unity 1 in numbers, noted I which is always squared

$$AI = IA = A$$

Determinant:

A determinant is a number that is associated with a square matrix. for example the matrix $\begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$

$$\begin{vmatrix} 1 & 2 \\ 2 & 3 \end{vmatrix} = 1 \cdot 3 - 2 \cdot 2 = -1$$

We have $\det(AB) = \det(A)\det(B)$. If $\det(A) = 0$ the matrix A is singular.

The sum of the diagonal element of a squared matrix A are trace: $Tr(A) = \sum_{i=1}^n a_{ii}$, a number which appears in many mathematical formulas. Some properties of the trace:

$$- Tr(AB) = Tr(BA)$$

Symmetric matrices:

A transpose of a matrix A is A^T that is $a_{ij} = a_{ji}$ (the rows become columns and the columns become rows). A matrix A is symmetric if

$$A^T = A$$

if we take the transpose and the conjugates of numbers of a matrix A we get the conjugate transpose $\bar{A}^T$ also noted A^* (note that $\overline{\bar{A}^T} = \bar{A}^T$). A matrix A is symmetric if $A = A^T$. If the matrix is self-adjoint or Hermitian¹⁷

$$A = \bar{A}^T$$

^[17] After French mathematician Charles **Hermite** (1822 – 1801) who studied them.

Applications:

Matrices are used in a lot of applications.

— If we take a vector function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ the derivative of f is a linear map seen in $f'(x + y) = f'(x) + f'(y)$ and $f'(ax) = af'(x)$. And the differential

$$d(f + g) = df + dg \quad \text{and} \quad d(af) = adf$$

The df presented by a matrix of partial derivatives the $m \times n$ **Jacobian** matrix J

$$\begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{bmatrix}$$

In the case $f : \mathbb{R} \rightarrow \mathbb{R}$ we get $J = [f']$.

If $m = 1$, J is just the gradient ∇f . If $\det(J) \neq 0$ then the inverse f^{-1} of f is smooth, so a **Jacobian** matrix of rank p . A map $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ is called smooth if all $\frac{\partial f}{\partial x_i}$ exist and are continuous, so we can do calculus on it. The df is a linear map associated with a matrix.

— We can present hyper-complex numbers by matrices. A complex number $x + iy$ is presented by the matrix $\begin{bmatrix} x & -y \\ y & x \end{bmatrix}$. We also can present a quaternion $ai + jb + ck + d$ is $\begin{bmatrix} ck + d & ai + jb \\ ai + jb & ck + d \end{bmatrix}$. or

$$\begin{bmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{bmatrix}$$



Examples:

— The set of invertible square matrices A , is a group called the linear group. If n is the order of the matrices it is noted $LG(\mathbb{R}, n)$, or $LG_n(\mathbb{R})$ where the field is $\mathbb{R}$. The law of composition is the matrix multiplication noted $\bullet$. It is a non-commutative group.

— The group of orthogonal matrices, called the group of orthogonal noted $O(n)$. An orthogonal A matrix is such that $A^{-1} = A^T$, we know that $\det(A) = \det(A^T)$. An orthogonal transformation preserves the inner product of vectors.

— The special orthogonal group: $SO(n)$ noted matrices an orthogonal matrix with $\det(A) = 1$.

The $SO(3)$ is group of rotations of Euclidean 3-space. The three groups $LG_n(\mathbb{R})$, $O(n)$ and $SO(n)$ are called topological groups.

— The unitary group: noted $U(n)$ is the group of unitary matrices matrix with $U^* = U$. The $SU(n)$ is the special group consisting in unitary U such that $\det(U) = 1$.

○ Integral Domains:

We see now an important type of rings.

We say that an element is zero divisor if $x * y = 0$ with neither $x = 0$ nor $y = 0$.

Definition:

An integral domain is a ring that has not zero divisors.

So

General ring $\rightarrow$ unitary ring $\rightarrow$ integral domain

Remark

— The collection of matrices with multiplication is not an integral domain. We have seen that the ring of matrices is not a domain because $AB = 0$ without A or B being zero matrix. As an example, for integer $n = 2$ we have for every real numbers a, b

$$\begin{bmatrix} a & b \\ a & b \end{bmatrix} \begin{bmatrix} b & b \\ -a & -a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

— In the ring $(\mathbb{Z}/4\mathbb{Z}, +, \cdot)$ we have $\dot{2} \cdot \dot{2} = \dot{0}$, so this ring is not an integral domain. We say that the element $\dot{2}$ is a zero divisor.

— Very important rings are the integral domains used in number theory ▲

Examples:

- $\mathbb{Z}$ is an integral domain.
- The ring $\mathcal{F}$ of functions on an interval I is not an integral domain.
- The set of numbers $a + ib$ where a and b are in $\mathbb{Z}$ is an integral domain. noted $\mathbb{Z} + i\mathbb{Z}$ or $\mathbb{Z}(i)$.
- The set of continuous function on an interval $[a, b]$ is not an integral ring. We can find two functions f, g such that $fg = 0$.

—The set of functions(not necessary continuous) on an interval $[a, b]$ is not an integral ring for the same reason▲

○ Ideals

The concept of “*Ideal*” comes from ideal numbers. Ideal numbers find origin in number theory related to the *Fermat Last Theorem*. When German Ernest **Kummer**(1810 – 1893) tried to solve this big problem, he faced a problem that unique factorization may fail. A known example is

$$6 = (1 + \sqrt{-5}) \cdot (1 + \sqrt{-5}) = 3 \cdot 2$$

So he introduced what is known as ideal numbers. **Kummer**'s solution is this : suppose we have the factorization $\alpha = \alpha_1 \alpha_2 = \alpha_3 \alpha_4$, in order to give the same factorization to α , we can introduce ideal factors such that : $\alpha_1 = p_1 p_2$, $\alpha_2 = p_3 p_4$, $\alpha_3 = p_1 p_3$, $\alpha_4 = p_2 p_4$ which gives

$$\alpha = p_1 p_2 p_3 p_4 = p_1 p_3 p_2 p_4$$

And the unique factorization is regained. As our example :

$$6 = \sqrt{2} \times \frac{(1 - \sqrt{-5})}{\sqrt{2}} \sqrt{2} \times \frac{(1 + \sqrt{-5})}{\sqrt{2}}$$

As $2 = \sqrt{2} \times \sqrt{2}$ and $3 = \frac{(1 - \sqrt{-5})}{\sqrt{2}} \times \frac{(1 + \sqrt{-5})}{\sqrt{2}}$. The number $\frac{(1 + \sqrt{-5})}{\sqrt{2}}$ is an ideal number.

where we can perform .

Ideals as sets one of the most important concept in modern algebra. It was German Richard **Dedekind** (1831 – 1916) who defined ideals in a ring in his *Tenth Supplement*¹⁸ (1871), in this theory Ideals in the ring of integers $\mathcal{O}_K$ are in place of integers of $\mathbb{Z}$.

Definition

¹⁸ They are supplements notes to the book of German Johann **Dirichlet**(1805 – 1859) : *Lectures on Number Theory*. After **Dirichlet** death, **Dedekind** began to edit the *Lectures* since 1863 adding his personal notes. The tenth supplement (Supplement) first appeared in the 1871 edition. Supplement X is now considered as one of the greatest texts in the history of mathematics, and in the words of number theorist Edmond **Landau**(1877 – 1938) : "It brought order to chaos and light to the deepest darkness". **Dirichlet's Lectures** have been translated (AMS, 1999) into English by Australian mathematician John **Stillwell** (1942–) without the supplements X and XI.

Let the set $\mathfrak{I} \subset \mathcal{R}$. We say that $\mathfrak{a}$ is an ideal if:

- $a, b \in \mathfrak{I}$ then, $a + b \in \mathfrak{I}$.
- $\forall c \in \mathcal{R}, a \in \mathfrak{I}$ then $ca \in \mathfrak{I}$.

An ideal is a part of a ring. Its origin is the set of multiples of an integer n in $\mathbb{Z}$ $n : n, 2n, 3n, 4n, \dots$. the set of the multiples of 5 is an ideal in $\mathbb{Z}$ noted $\langle 5 \rangle$ this ideal is the set :

$$\langle 5 \rangle = \{0, 5, 10, 15, 20, 25, 30, \dots\}$$

In the ring $\mathbb{Z}$, $\{0\}$ and $\mathbb{Z}$ are trivial ideals. An ideal that is not trivial is proper. The set of the multiples of 3 is a proper ideal of $\mathbb{Z}$.

$$\langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18, \dots\}$$

It is equivalent to say that a proper ideal is not one of the two $\langle 0 \rangle$ or $\langle 1 \rangle$ for we have :

$$\{0\} = \langle 0 \rangle \quad \wedge \quad \mathcal{R} = \langle 1 \rangle$$

Remark

- A similar structure to ideals is the divisor structure due to German Leopold **Kronecker** (1823 — 1891).
- Any integral domain $\mathcal{R}$ has two trivial ideals : $\{0\}$ and $\mathcal{R}$.

Example:

- Every ring is an ideal, it is a trivial ideal.
- We have

$$\mathbb{Z} = \langle 1 \rangle = \{\dots, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, \dots\}$$

is a ideal.

- $\langle 2, 3 \rangle$ is an ideal in $\mathbb{Z}$, it contains all the integers of the form $2a + 3b$ and we observe that

$$\langle 2, 3 \rangle = \langle 1 \rangle = \mathbb{Z} \quad \blacktriangle$$

Dedekind in the previous example as $2 = \sqrt{2} \times \sqrt{2}$ and $3 = \frac{(1-\sqrt{-5})}{\sqrt{2}} \times \frac{(1+\sqrt{-5})}{\sqrt{2}}$. The number $\frac{(1+\sqrt{-5})}{\sqrt{2}}$ is an ideal number.

An ideal is maximal if it contains all the ideals. It is the biggest proper ideal by inclusion.

Principal Ideals:

Dedekind says that an ideal $\mathfrak{I}_1$ divides $\mathfrak{I}_2$ if $\mathfrak{I}_2 \subset \mathfrak{I}_1$, $\mathfrak{I}_2$ is a divisor of $\mathfrak{I}_1$. An ideal $\mathfrak{I}$ of a ring $\mathcal{R}$ is a prime ideal if its divisors are $\mathcal{R}$ and $\mathfrak{I}$ only. To say that $a|b$ like saying $\mathfrak{I}_b \subset \mathfrak{I}_a$.

Definition

Let the an ideal $\mathfrak{I} \subset \mathcal{R}$. We say that $\mathfrak{I}$ is a principal ideal if: it is generated by a single element. The ring in which every ideal is principal is principal ring.

Example:

— in $\mathbb{Z}$, every ideal is principal. The ideal

$$5\mathbb{Z} = \langle 5 \rangle = \{\dots, -5, 0, 5, 10, 15, 20, \dots\}$$

is principal.



A domain where every ideal is a principal ideal domain (PID).

Quotient Ring:

Let I an ideal we define a quotient ring $\mathcal{R}/I$

Polynomials

Another ring that is important is the ring of polynomial. A polynomial is a

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

Ideals are a form from.

Polynomials in $\mathbb{Z}_n$

The coefficients of polynomial can be in $\mathbb{Z}_n$ for example consider the polynomials in $\mathbb{Z}_8$: $2x + 6$ and $2x^2 + 3x + 5$, the product is

$$(2x + 6)(2x^2 + 3x + 5) = 4x^3 + 4x^2 + 4x + 7$$

○ Modules

Now we know vector spaces, a module is just a vector space but in place of the field K we put a ring $\mathcal{R}$. After we have the module is like a vector space.

Modules are generalization of vector spaces. Instead of a field, the scalars are from a ring which may be not commutative. Modules are used a lot in algebraic geometry where we and also in algebraic topology.

Definition

Let $\mathcal{R}$ a ring. We say that $\mathfrak{a}$ is a module if:

- $(a + b)x = a(b + x)$.
- $(a + b)x = ax + bx$.
- $1x = x$.

We can define right $\mathcal{R}$ -module and left $\mathcal{R}$ -module. If $\mathcal{R}$ is commutative then right $\mathcal{R}$ -module and left $\mathcal{R}$ -module are the same.

Remark

- A module can have no base unlike a vector space.
- Any integral $\blacktriangle$

Example:

- Every ring $\mathcal{R}$ is a $\mathcal{R}$ -module. $\blacktriangle$

Exercises

- 1) Show that $\mathcal{R} = \{0\}$ is a ring.
- 1) is the set $(\mathbb{C}, +, \bullet)$ is a ring ?
- 1) if $(\mathcal{R}, +, \bullet)$ is a ring then $a \times 0 = 0$.
- 1) show that $\{0\}$ is an ideal in a ring.
- 1) let A be an orthogonal matrix. Show that $\det(A) = \pm 1$
- 1) Show that : $\det(A^T A) \geq 0$.
- 1) Find the determinant of the matrix $A = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \\ 2 & 0 & 1 \end{bmatrix}$ by four methods.

1) what is the solution of $AX = 0$ if $\det(A) \neq 0$?

1) are the following matrices orthogonal ?

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

1) Let A be an orthogonal matrix. Show that $\det(A) = \pm 1$

1) find the determinant of the matrix $\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \\ 2 & 0 & 1 \end{bmatrix}$ by four methods.

1) Show that $\det(A^{-1}) = \frac{1}{\det(A)}$. What do you infer?

1) what is the complex number presented by $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$?

1) Show that any real symmetric matrix is **Hermitian**.

1) show that the eigenvalues of $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ are a and b .

Fields

Roughly, a field is a set like $\mathbb{R}$, where we can perform all the usual operations we are used to and remain at the same time in the set. The first field was studied by French Evariste **Galois** with his work on algebraic equations. During the *XIX* century, German school produced a lot of original work on algebraic fields and a lot of result in algebraic number theory. In 1910, German mathematician Ernst **Steinitz** (1871 – 1928) published his classical “*Algebraic Theory of Fields*” where he gathered previous results about fields in a unified text that prefigured the beginning of modern algebra.



Steinitz

○ Definition of a Field

Definition:

Let $\mathcal{K}$ a set elements with two internal operations $*$ and $\diamond$ the is a field if:

- $(\mathcal{K}, *)$ is an abelian group.
- $(\mathcal{K}, \diamond)$ is a group.
- $\diamond$ is distribution of on : $a \diamond (b * c)$

So a field $(\mathcal{K}, *, \diamond)$ has two laws of composition, is composed of two groups the first $(\mathcal{K}, *)$ which is **abelian**, and the second $(\mathcal{K}, \diamond)$ which is not necessary **abelian**.

Remark

- German Richard **Dedekind** (1831 – 1916) introduced the word *Körper* in 1871 from which we have the letter $\mathcal{K}$.
- Every field is a ring. Every field contains a unitary integral domain and every ring contains an **abelian** group.
- Every subring of field is an integral ring.

- It is easy to show that a field cannot have a proper ideal.
- we add the condition that $0 \neq 1$.
- If the second law $\diamond$ is not commutative, the structure is a skew field or a division ring. An example is due to English scientist William **Hamilton** (1805 – 1865) with his quaternions. Mathematicians wanted to find numbers represent rotations in 3 – dimension spaces $\mathbb{R}^3$ like complex number present rotations in $\mathbb{R}^2$, but that was impossible. **Hamilton** moved to $n = 4$ ($\mathbb{R}^4$) and introduced his quaternions, they are number of the form $ai + bj + ck + d$ where

$$i^2 = j^2 = k^2 = -1$$

and $a, b, c, d \in \mathbb{R}$. The multiplication is indeed non abelian : $ij = -ji$... The set of quaternions $(\mathbb{H}, +, \bullet)$ is a skew field, $\times$ is not commutative. John **Milnor** made an exotic sphere S^7 gluing $S^3 \times D^4$ with quaternions multiplication.

After that people got interested in numbers like complex and quaternions called hypercomplex systems. it was first showed that the cases $n = 5, 6$ and 7 are impossible. For $n = 8$ there exist a system invented independently by John **Graves** (1806 – 1870) and **Cayley** that does not verify associativity : the octonions $(\mathbb{O}, +, \bullet)$. In 1863, German mathematician Karl **Weierstrass** (1805 – 189) showed that $\mathbb{C}$ is the more general abelian field from $\mathbb{R}$ $\blacktriangle$

Examples:

- The sets $(\mathbb{Q}, +, \bullet)$, $(\mathbb{R}, +, \bullet)$, and $(\mathbb{C}, +, \bullet)$ are abelian fields. $\mathbb{Z}$ is a subring of the field $\mathbb{Q}$.
- the ring $\mathbb{Z}/n\mathbb{Z}$ is a field if $n = p$ a prime number.
- When we take the complex roots of 1 and we have a new field called algebraic field $\mathbb{Q}(\zeta_p)$ are very important in number theory. We know that integer $n = p_1 p_2$ the same in $\blacktriangle$

a very important is : the is that is algebraically close any has solution of coefficients in $\mathcal{K}$ inside $\mathcal{K}$ itself.

Theorem

Every algebraic equation of degree n has n roots in $\mathbb{C}$.

A characteristic of a field is an integer n such that $a^n = 1$.

Finite Fields

Fields can be finite or infinite. A finite field is a field that has a finite number of elements. In his work on algebraic equations, **Galois** a fields but finite fields. **Galois** has all finite fields.

Theorem:

If K is a finite field then $\#(K) = q = p^n$.

Also or this we note a finite field usually by the symbol $\mathbb{F}_q$

Remark

—a finite field is usually called a **Galois field** ▲

Examples:

—Some fields are finite and very interesting. The set $\mathbb{Z}/n\mathbb{Z}$ is a field iff n is a prime, it is a field with p elements. So $\# \left(\frac{\mathbb{Z}}{p\mathbb{Z}} \right) = q = p^1$.

—The solution of a algebraic equation is an algebraic number, the set $\mathbb{A}$ of algebraic numbers is a field, whereas the set of transcendental number is not a field ▲

Theorem

Every finite field is commutative.

A proof of this fact was published by Scottish mathematician Joseph **Wedderburn** (1882 – 1948) in 1905. This means that if a field is not **abelian** so it is infinite. The sets $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are infinite fields under $+$ and $\cdot$ as well as the field $\mathbb{A}$ of algebraic numbers. We have a sequence of fields inclusions: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ and $\mathbb{Q} \subset \mathbb{A} \subset \mathbb{C}$. Any infinite field we will study contains $\mathbb{Q}$ as a subfield. The field $\mathbb{Q}$ has not a field in it, it is a prime field. We not a finite field with the symbol $\mathbb{F}_q$.

○ Vector spaces

After we have seen the module structure in ring theory, we will see a similar structure that is very important in mathematics which is a vector space called also linear space. A $\mathcal{K}$ –vector space V is a special module, it is a structure that used much in mathematics.

Definition:

- $(V, *)$ is an **abelian** group.
- $\forall a, b \in \mathcal{K}$ we have $x, y \in V$:
- $(x + y)a = xa + ya$.
- $(a + b)x = ax + bx$.
- $a(bx) = (ab)x$.
- $1x = x$ $1 \in \mathcal{K}$.

The same way we define when $\mathcal{K}$ is $\mathbb{C}$. The elements of a vector space are vectors. we can be a vector a general sense or a function. vectors are linearly independent if

$$a_1 v_1 + a_2 v_2 + \dots + a_n v_n = 0$$

This implies that all $a_1 = a_2 = \dots = 0$. two vectors a, b are linearly independent iff $a \times b \neq 0$.

Examples:

- Every abelian field is a vector space over itself.
- $\mathbb{R}^n$ are all vector spaces over $\mathbb{R}$.
- $\mathbb{C}^n$ are all vector spaces over $\mathbb{R}$.
- The set of quaternions $\mathbb{H}$ is a vector space of basis $(1, a, b, c)$ over $\mathbb{R}$.
- The set of convergent series is a vector space over $\mathbb{R}$.
- the set of continuous functions is a vector space over $\mathbb{R}$ $\blacktriangle$

Quotient space:

The direct product of two vector spaces V_1 and V_2

$$V_1 \oplus V_2 = \{(u, v) : u \in V_1, v \in V_2\}$$

Let V_1 be a vector space and V_2 another vector subspace such that $V_2 \subset V_1$. We can a quotient by finding an equivalence relation so we define the V_1/V_2 which is a vector space, so of equivalence classes.

Examples:

- Let $V = \mathbb{R}^2$ and l a line in the plan V . The quotient space V/l is the set of lines parallel to l . So two lines l_1 and l_2 are equivalent modulo l : the line l_1 is equivalent to the line l_2 modulo l , and we write $l_1 \sim l_2$.

- linear.



Basis:

A basis $\mathcal{B}$ is a set of vectors $b_1, \dots, b_n$ such that verify :

Definition:

- they are linearly independent.
- every vector in V can be written as a linear combination of the vectors of $\mathcal{B}$.

Remark

- when the dimension of V is the same as the basis n to that is a basis it suffices to prove that $\det(A) \neq 0$ ▲

We have this difficult theorem:

Definition:

Every vector space V has a basis.

For proving this result is difficult.

Tensor product of vector spaces:

We have seen some products.

The tensor product of two vectors is $v_1 \otimes v_2 = v_1 v_2^T$, so the result is a matrix. Sometimes the matrix is written as a vector so the tensor product is the product between the elements of the two vectors :

$$v_1(a, b) \otimes v_2(c, d) = v_3(ac, ad, bc, bd)$$

It has some properties.

Theorem:

Proof:

The tensor product of vector spaces of m, n is a vector space of dimension $n \cdot m$.

○ Linear maps

After linear function between them. We can say map or mapping.

Definition:

- $f(x + y) = f(x) + f(y)$
- $f(ax) = af(x)$

the condition can be resumed to : f is linear if $f(ax + by) = af(x) + bf(y)$. A linear map is a type of homomorphism (or morphism). An important result in linear algebra is

Theorem:

Any linear map from $\mathbb{R}^m$ to $\mathbb{R}^n$ and every is associated with a matrix of $n \times m$.

Examples:

- A differential df is a linear map.
- linear maps are the subject of functional analysis.



○ Linear Systems Revisited

After linear function we system of linear and expose some important matrices. These from many practical situation in science in general. Let take the simplest example of $n = 2$

$$\begin{aligned}x + y &= 2 \\x - y &= 1\end{aligned}$$

The linear system can be simplified by

$$AX = Y$$

Where Y is a given vector and $X = (x, y)$ the unknown vector of in a certain field like $\mathbb{R}$. to the system we to a triangular or echelon form.

When $n = m$ The system $AX = Y$ has three:

- if $\det(A) = 0$ there is a unique solution.
- if $\det(A) \neq 0$ then either no solution or infinity of solutions.

The general linear system $n = 2$

$$\begin{aligned} ax + by &= e \\ cx + dy &= f \end{aligned}$$

And to facilitates the solution we used the augmented matrix for example

$$\begin{bmatrix} a & b & e \\ c & d & f \end{bmatrix}$$

To solve systems of linear equations we use many methods like Gauss elimination, which leads to a row echelon form. Take an example

$$\begin{aligned} 2x + 3y + 2z &= -3 \\ 2x + 3y + 5z &= 2 \\ x + 3y + 2z &= 2 \end{aligned}$$

becomes

$$\begin{bmatrix} 2 & 3 & 2 & -3 \\ 2 & 3 & 5 & 2 \\ 1 & 3 & 2 & 2 \end{bmatrix}$$

and Gauss method or Jordan method that to reduced row-echelon form

$$\begin{bmatrix} 1 & 0 & 0 & -3 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \end{bmatrix}$$

Inverse of a matrix

A matrix can have an inverse (like real $a \neq 0$ has for inverse $\frac{1}{a}$).

$$AA^{-1} = I$$

The inverse is unique. In the previous methods we did not use the inverse of a matrix. In general if $\det(A) \neq 0$ the solution

$$AX = Y \Rightarrow X = A^{-1}Y$$

where A^{-1} is the inverse of A .

An inverse of a matrix is a matrix A^{-1} such that $AA^{-1} = I_n$. Where I_n is the identity matrix, when $n = 2$ it is

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

A matrix that has an inverse is nonsingular, otherwise it is singular.

Special matrices

An orthogonal matrix A is a matrix such that

$$A^{-1} = A^T$$

The orthogonal matrices have for determinant one of the umbers

$$-1, \quad 1$$

orthogonal matrices are rotations they preserve and change the direction which gives a rotation. There are also unitary matrices.

A unitary matrix A is a matrix whose inverse is its conjugate transpose, so a matrix A is unitary if

$$A^{-1} = A^* = \bar{A}^T$$

Every real orthogonal matrix is unitary. The unitary matrices have for determinant one of the umbers

$$-1, \quad 1, \quad i, \quad -i$$

We have until now

$$\begin{array}{ll} \text{symmetric} & \leftrightarrow \text{Hermitian} \\ \text{orthogonal} & \leftrightarrow \text{unitay} \end{array}$$

Eigenvalues

An interesting propriety of squared matrices is their eigenvalues. We say that the number λ is an eigenvalue for A if it verifies the equation $Ax = \lambda x$. To find the eigenvalues of a matrix A we solve the equation

$$\det(A - \lambda I) = 0$$

Some matrices have no eigenvalues. The product of the eigenvalues of a matrix A is its determinant, and the sum is the trace of A .

For every eigenvalue there is eigenvector $Ax = \lambda x$, x is the eigenvector associated with the eigenvalue λ . A theorem due to **Hermite** says that all eigenvalues of symmetric matrices are real. We have seen that the inverse of a matrix A is A^{-1} such that $AA^{-1} = I$.

The eigenvalues of matrices play an important role in quantum mechanics, exactly through eigenvalue problem

$$Ax = \lambda x$$

A is a linear operator and it is very important to find the eigenvalues and eigenvectors.

—If we a vector function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ the derivative is the Hessian matrix¹⁹

$$\begin{bmatrix} u_{xx} & u_{xy} \\ u_{yx} & u_{yy} \end{bmatrix}$$

It is a symmetric matrix. The eigenvalues of H that the curvature of the surface.

○ Algebraic Fields

An interesting fields studied in the theory of numbers that use algebraic proprieties. To first we see what an extension is. The field extension of a field K is another greater such that . We have $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ three fields : $\mathbb{C}$ is the extension of $\mathbb{R}$, $\mathbb{R}$ is the extension of $\mathbb{Q}$. We have seen that the field $\mathbb{Q}$ has not a field in it, it is a prime field. We by the symbol

$$K/\mathbb{Q}$$

¹⁹ Due to German Ludwig **Hesse**(1811 – 1874).

An interesting extension field is $\mathbb{Q}(\sqrt{5})$ numbers of the form $a + b\sqrt{5}$ $a, b \in \mathbb{Q}$ it is an extension of $\mathbb{Q}$ because $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5})$, we find $\mathbb{Q}$ when $b = 0$.

An algebraic field is a field whose elements are of the form $a + b\sqrt{D}$, these numbers are algebraic numbers that mean they came from algebraic equations. The numbers a, b can be in $\mathbb{Z}$ the field is noted $\mathbb{Z}(\sqrt{D})$ or in $\mathbb{Q}$, the field is noted $\mathbb{Q}(\sqrt{D})$. So formally:

Definition:

A number field $\mathbb{Q}(\sqrt{D})$ is a finite extension of the field $\mathbb{Q}$.

It is a set of number of the form $a + b\sqrt{D}$ as vector space is finite (in $a + b\sqrt{D}$ the is 2 and for $a + b\sqrt{D_1} + c\sqrt{D_2}$ is 3).

Remark

— an a book *the theory of algebraic numbers* by **Hilbert** in 1897 . algebraic numbers of order 1 are the rationals $\mathbb{Q}$. algebraic integers of order 1 are the integers , algebraic integer of order 2 are the Gauss integers of the form $a + ib$.▲

Examples:

- If α is an algebraic number then is an algebraic field. Some $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, ... are algebraic fields.
- Some fields of function of variable like the field of rational Function $\mathcal{K}(x)$ and field of rational functions with two variables $\mathcal{K}(x, y)$. This was very fruitful in number theory and proved the Riemann hypothesis²⁰. Let the rational function field $K[x]$ the polynomial ring $K(x)$ is a subring in the same way that $\mathbb{Z}$ is subring of $\mathbb{Q}$.
- The big **Birch—Swininter—Dyer** conjecture is about elliptic curves over an algebraic field K . It says: the rank of an abelian group ▲

Integers, units and primes:

When we generalize the proprieties to these fields new thing appear.

-there are numbers inside the ring play the role of integers $\mathbb{Z}$ in a ring inside called the ring of integers noted $\mathcal{O}$.

-in a field every element that has an inverse for the second law of composition, it is called invertible

²⁰ See Peter **Roquette**(1927 – 2023) *The Riemann hypothesis for characteristic p* (Springer 2018).

or a unit. The set of units $U(\quad)$ constitutes a group to the second operation, we have:

$$U(\mathbb{Z}) = \{-1, 1\}.$$

$$U(\mathbb{R}) = \mathbb{R}^*.$$

$$U(\mathbb{Q}) = \mathbb{Q}^*.$$

$$U(\mathbb{C}) = \mathbb{C}^*$$

An studies is to find primes, units, unique factorization domains,...with a lot of open problems.

Definition

An element α in the field is a prime if:

-it is neither 0 nor a unit.

-if $\alpha|ab$ then $\alpha|a$ or $\alpha|b$.

In $\mathbb{Z}$ prime is synonym of irreducible but in general this is not true. Prime is irreducible but if irreducible not that is prime. To that is irreducible we introduce the norm N , so we have $N(\alpha\beta) = N(\alpha)N(\beta)$. for example

$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2D$$

Unique Factorization:

It is the main subject of algebraic number theory²¹, to find integers, primes and units. which has given a fecund generalization the usual integers. We have seen (PID) and relationship with the uniqueness of factorization

-every is UFD

-every is UFD

-every is UFD

An example of not UFD is the field $\mathbb{Q}(\sqrt{5})$ studied by German Richard **Dedekind**.

Galois Theory:

As it is known Galois work is situated into the efforts to find formula to algebraic equation when 5. From that stemmed what mathematician call Galois theory, a modern theory not only in algebraic equation but in group representation, number theory and even topology. As Dutch Bartel van **Waerden**(1903 – 1996) formulated it

²¹ A good introduction to this domain is *Introduction to Algebraic Number Theory* by Şaban **Alaca** and Kenneth **Williams**.

Modern algebra begins with Evariste Galois. With Galois, the character of algebra changed radically. Before Galois, the efforts of algebraists were mainly directed towards the solutions of algebraic equations...he was the first to investigate the structure of fields and groups, and he showed that these two structures are closely connected. If one wants to know whether an equation can be solved by radicals, one has to analyze the structure of its Galois group. After Galois, the efforts of the leading algebraists were mainly directed towards the investigation of the structure of rings, fields, algebras and the like.

An important note here is we find relation with:

- existence of solutions by radical to a polynomial equation $P_n(x) = 0$.
- trisection of the angle
- the of by compass and ruler.

Splitting fields:

Let be a polynomial equation $P_n(x) = 0$ we want to solutions in $\mathbb{R}$ or $\mathbb{C}$. let the equation . every has a Galois group G constituted of the solution of the equation

Here the splitting field is the smallest extension field that contains the solutions. The word splitting comes from that fact the polynomial $P_n(x)$ splits in linear factors $(x - a_i)$.

we know that automorphism is a bijection from a set E in itself. What does the automorphism preserve here?

The solvable group:

Let : $\{e\} \triangleleft G_n \triangleleft \dots \triangleleft G_1 \triangleleft G$

Examples:

- every abelian group is solvable : $\{e\} \triangleleft G$.

Algebras

In the structure of a vector space, the first operation between vectors constitutes a group but the second operation is defined between scalars and vectors. In an algebra the first operation is like a vector space, but the second operation can be defined between vectors themselves.

Definition:

Let V a vector space over a field K

- $(V, +)$ is a group.
- $(V, \times)$ is

A lot of number systems after the complex number with strange behavior and they have been seen to as algebras.

Remark

- an algebra can be associative or not▲

Examples:

- the set $(\mathbb{R}, +, \cdot)$ is an algebra.
- the set $(\mathbb{C}, +, \cdot)$ is an algebra.
- **Banach** algebras are important in functional analysis.
- the set $(\mathbb{H}, +, \cdot)$ of quaternions is an algebra, it is the first non-**abelian** algebra▲

we have

Frobenius theorem(1877):

Any finite dimension associative algebra is isomorphic to one of the three algebras: $\mathbb{R}, \mathbb{C}$ or $\mathbb{H}$. So $\mathbb{H}$ is the only real- finite dimension algebra.

Clifford algebra:

Hypercomplex numbers that resulted in the attempt to complex numbers $a + iy$ in a new structures.
Let V a vector space over a field K .

Lie algebra:

We have seen in the chapter about groups the important concept of Lie groups. A Lie algebra is a vector space V noted often $\mathfrak{g}$ and with called the Lie bracket which the following conditions:

- bilinear.
- alternative.
- verifies Jacobi identity.

The relation between the two is : every Lie group a tangent space at the identity.

We have seen group and that one important are Lie groups. A group $(G, *)$ called **Lie** group, In a group $(\mathbb{R}, +)$ we to another element, but **Lie** group²² is different it implies a continuous law of transformation , it is a function. $(G, *)$ is itself a manifold, and the operation is continuous so it is a topological group.

So $(G, *)$ is a **Lie** group

- G is a manifold
- for every $g_1, g_2 \in G$, $g_1 * g_2$ is smooth

²² In fact a Lie group is a topological group, where is not only continuous but differentiable as well.

– the map $g \rightarrow g^{-1}$ is smooth

Both $(\mathbb{R}, +)$ and $(\mathbb{R}, \bullet)$ are Lie groups. The idea of **Lie** was to use group theory to solve differential equations.

An example of a Lie group is the group of rotations in $\mathbb{R}^3$ noted $O(3)$ the rotations are continuous, thus we consider the group a manifold.

every Lie give raise to a Lie algebra. an algebra is like a linear space $(E, +, \bullet)$ where is also .
A Lie algebra is with the Lie bracket of vector fields x and y :

$$[x, y] = xy - yx$$

Modern differential geometry is based on the fiber bundle theory.

Examples:

– for $f(x) = x$ is linear from to its ker is simply and thus it is injective.



Exercises

1) Show that the following sets are not fields:

– $(\mathbb{Z}, +, \bullet)$.

– $(\mathbb{Q}, +, \bullet)$.

–

1) show that $1 + i$, $\frac{i}{2}$ and $\sqrt{3} + i\sqrt{2}$ are algebraic numbers.

1) How many solutions the equation $x^4 + 3x^2 - 4 = 0$ has ? Find them.

1) Show that the set $\mathbb{T}$ of transcendental numbers is not a field.

1) Is $(\mathbb{Q}^*, +, \bullet)$ a field?

1) Show that a field cannot have zero divisors.

1) Every finite domain (ring) is a field. What do you infer?

1) show that a field cannot have a proper ideal.

1) Show that the components of a vector in a basis are unique.

1) Show that n vectors contains k linearly dependent it is dependent itself.

1) show that n vectors are dependent iff one of them is a linear combination of the others.

1) Show that $\{0\}$ is a vector space. What is its dimension?

1) Show that 2 vectors in the plan are dependent iff they are parallel.

1) Say if the following vectors are independent :

i) $(1, 2)$, $(0, 0)$ in $\mathbb{R}^2$.

ii) $(1, 2, 1)$, $(0, 2, 3)$, $(1, 2, 3)$ in $\mathbb{R}^3$.

1) show that 4 vectors in $\mathbb{R}^3$ are dependent.

- 1) find the polynomial $ax^2 + bx + c$ passing by the points : $(1,2)$, $(-2,3)$.
- 1) Show that two vectors a, b are linearly dependent iff $a \times b = 0$ (contraposition).
- 1) From $k^2 = -1$ in quaternions, show that $ij \neq ji$.
- 1) let q_1 and q_2 two quaternions. Show that $q_1 q_2 = v_1 \circ v_2 + v_1 \times v_2$.
- 1) show that $\text{Ker}(f) = \{0\}$ iff f is injective.
- 1) Let ϕ be a morphism, show that if : $g \in \text{Ker}(\phi)$ then $g^{-1} \in \text{Ker}(\phi)$.
- 1) Let f linear. Show that $f(0) = 0$.
- 1) Let f linear. Show that : $\text{Ker} f = \{0\} \Rightarrow f$ is injective.
- 1) Find $\begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix}^{-1}$ by three methods.
- 1) Show that any real orthogonal matrix is unitary.
- 1) show that very real symmetric matrix is Hermitian.
- 1) Show that if λ is an eigenvalue for A , then λ^{-1} is an eigenvalue for A^{-1} .
- 1) A matrix A is singular iff 0 is a root of its minimal polynomial. By two methods show that $\begin{vmatrix} -2 & 8 \\ -1 & 4 \end{vmatrix}$ is singular.
- 1) find $\begin{bmatrix} 1 & 4 \\ 2 & 7 \end{bmatrix}^{-1}$ by three methods(inverse by row reduction).
- 1) find the spectrum of $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. How to get them real?
- 1) Show that the vector $\mathbf{0}$ is dependent.
- 1) show that the set of orthogonal vectors e_1, e_2, e_3 (eins) is independent.
- 1) write the equation of plane passing the points $a(1,2,2), b(1,1,1)$ and $c(2,0,-1)$.
- 1) find the direction cosines if $a = e_1 - 2e_2 + 5e_3$
- 1) show that $a \times (b \times c) \neq (a \times b) \times c$.
- 1) what about $ax + by = c$?
- 1) solve the equation

$$\begin{cases} x - 3y = 4 \\ -2x + 6y = -8 \end{cases}$$

it has an infinity of solutions (degenerate equation). Give the general solution.

- 1) solve by Gauss elimination

$$\begin{cases} x + y = 2 \\ 2x + y = 3 \end{cases}$$

- 1) write the Cauchy-Schwarz inequality in terms of dot product.
- 1) let (e_1, e_2, e_3) a basis(Hamel) and $v_j = \sum_{i=1}^3 a_{ij} e_i$. when (v_1, v_2, v_3) is a basis ?
- 1) What is a Schauder basis (think of $[0,1]$) ?
- 1) let $a(1,2,2), b(1,1,1)$ by Gram-Schmidt method.
- 1) Let f linear, show that it is continuous at every x .
- 1) Let f linear, show that if it is continuous at every x it is at 0.
- 1) derivate a linear function f .
- 1) minor and rank .
- 1) Discuss the solution of $Ax = b$. What about $Ax = \mathbf{0}$? Interpretation when $n = 2,3$.
- 1) a linear function f is represented by A . when is f not one-to-one?
- 1) define an orthogonal transformation(rigid (preserves):rotation, reflection).

1) find the comatrix then adjugate C^T of every matrix

$$\begin{bmatrix} 1 & 3 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 4 \\ 1 & 2 \end{bmatrix}, \quad \begin{bmatrix} 1 & 3 \\ 1 & 2 \end{bmatrix}$$

1) find the adjoint

1) $I = [\delta_{ij}]$. Find the inverse of : $\begin{bmatrix} 1 & 3 \\ 1 & 1 \end{bmatrix}$. A linear non-singular map is “affine”.

1) $A(BC) = (AB)C$. $\det(kA) = k^n \det(A)$.

1) calculate the determinant the following matrix by three methods

$$\begin{bmatrix} 1 & 0 & 1 \\ 2 & 1 & 0 \\ 0 & 3 & 1 \end{bmatrix}$$

1) inverse by row reduction

1) Explain $Av = \lambda v$.

1) what relation between $\text{spectrum}(A)$, $\det(A)$ and $\text{Tr}(A)$.

1) what if one $\lambda = 0$?

1) Show that λ is a eigenvalue of A , then λ^{-1} is an eigenvalue for A^{-1} .

1) find the eigenvalue and eigenvectors of the following matrices

$$\begin{bmatrix} -1 & 4 \\ -2 & 5 \end{bmatrix}, \quad \begin{bmatrix} 1 & -1 \\ 2 & 4 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 4 & 1 \end{bmatrix}$$

1) find the eigenvalue of the following matrices

$$\begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix}, \quad \begin{bmatrix} -i & 0 \\ 0 & -i \end{bmatrix}$$

1) what about the following matrix $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. What is the spectral radius $\rho(A)$?

1) let A be symmetric non-singular. Show that A^{-1} is also symmetric.

1) Show that every real symmetric matrix is **Hermitian**(self-adjoint).

1) **Pauli** introduced his matrices

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Show that they are **Hermitian**.

1) find the eigenvalues of **Pauli** matrices.

1) Let $a \neq 0$ find the eigenvalue and eigenvectors of the following matrix

$$\begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{bmatrix}$$

1) why the matrix $\begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{bmatrix}$ has no eigenvectors ?

1) show the Cayley–Hamilton theorem (due to Fröbenius) for the matrix : $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

1) Show that A^{-1} is unique.

1) Show that $(AB)^{-1} = B^{-1}A^{-1}$.

1) why is the matrix $\begin{bmatrix} \cos(x) & -\sin(x) \\ \sin(x) & \cos(x) \end{bmatrix}$ a rotation ?

1) are the following matrices unitary ?

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

1) show that every real orthogonal matrix is unitary.

1) is it true : if $\det(A) = 1$ then A is orthogonal?

1) is it true : if $\det(A) = 1$ then A is special unitary?

1) let $A = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ i & -i \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$, show that it is unitary. Calculate its determinant.

1) what are the possible values of the determinant of a unitary matrix? what is $SU(n)$?

1) show that the following matrices are diagonalizable

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

1) show that every symmetric matrix is diagonalizable.

1) Let A and B similar. Show that $\det(A) = \det(B)$.

1) of what is composed D ?

1) Jordan form. Every square matrix is similar to a normal Jordan form. $\therefore$ (then...)



Open Problems

A lot of problems in abstract algebra (as group theory) has been posed in Russian academia circles during the Soviet era and the search for solutions continues until now. There exists in particular two lists called *notebooks*:

—The Kourovka Notebook.

since 1965 in what is known as the first copy was a handwritten copy composed on the 16th of February 1965. The name of the collection of problems derives from the Kourovka Tourist Center near Sverdlovsk (Russia), where the first All-Union Symposium on Group Theory took place. The idea of the Kourovka Notebook was suggested by Russian mathematician Mikhail **Kargapolov** (1928 – 1976) during the preparations for the Symposium. Up to now 2026 many versions with new problems and solves one (the seventh edition in 1983 at AMS). A new version from the university of Novosibirsk (Russia) is online.

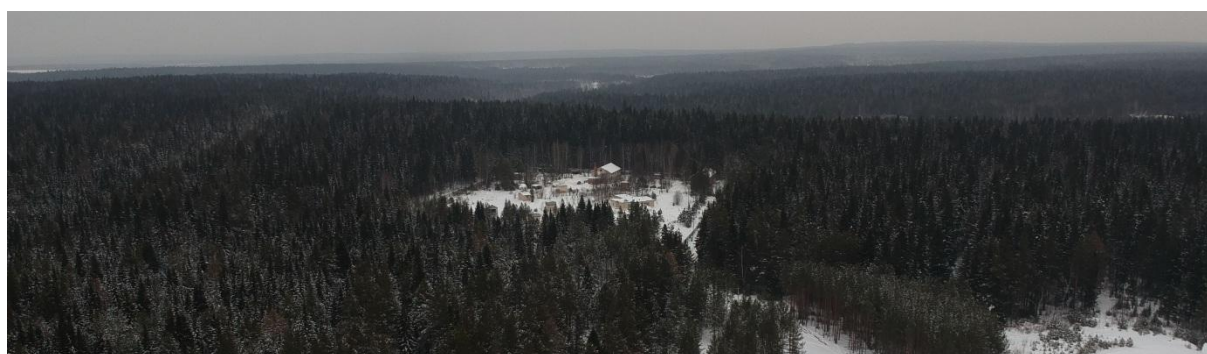
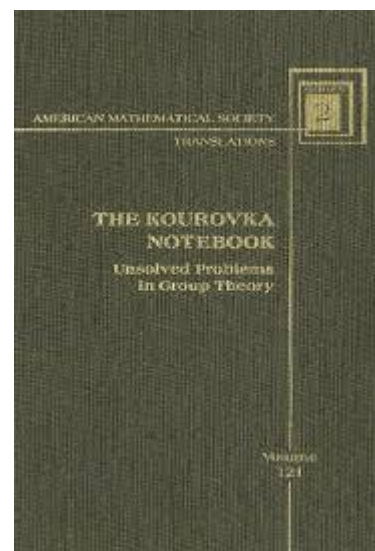


Fig. Kourovka Observatory.

— the Sverdlovsk Notebook

Another reference began since 1966 by Lev **Shevrin** (1935–) and researchers around him at the Ural State University. The city Sverdlovsk is now called Yekaterinburg, the three were enriched by under of algebraist P. G. **Kontorovich** (1905– 1968). The problems around algebraic Systems.

-The Cherlin—Zilber conjecture(1979).

